Perancangan Inisial Permutasi dengan Prinsip Lotre dalam Menahan Kriptanalisis *Known Plaintext Attack* (KPA) pada Kriptografi *Hill Cipher*

[1)]Muhammad Roikhan, [2)]Alz Danny Wowor
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50771, Indonesia
Email: [1)]672010104@student.uksw.edu, [2)]alzdanny.wowor@staff.uksw.edu

Abstract

Security is the most important aspect in data communications. Hill cipher is a technique of chryptography that can be used to secure data or information. However, Hill Cipher which only have 26 characters as the input of plaintext is easily solved with a known plaintext attack (KPA) cryptanalysis techniques using matrix multiplication. Therefore, in this study will be made a new technique that is not easily solved with a known plaintext attack in the form of Initial Permutations with Principle Lottery using 256 characters. The results showed that this algorithm has a fairly low correlation values between plaintext and ciphertext. Modifications Hill Cipher can also withstand attacks cryptanalysis known plaintext attack (KPA).

***Keywords**: Hill Cipher, Chryptography, Matrix, Initial Permutations, Lottery, Known Plaintext Attack*

Abstrak

Keamanan adalah aspek paling penting dalam komunikasi data. *Hill cipher* merupakan sebuah teknik kriptografi yang dapat digunakan untuk mengamankan data atau informasi. Namun, *Hill Cipher* yang hanya mempunyai 26 karakter sebagai masukan plainteks mudah dipecahkan dengan teknik kriptanalisis *known plaintext attack* (KPA) menggunakan perkalian matriks. Oleh sebab itu, pada penelitian ini akan dibuat sebuah teknik baru agar tidak mudah dipecahkan dengan known plaintext attack berupa Inisial Permutasi dengan Prinsip Lotre menggunakan 256 karakter. Hasil penelitian menunjukkan bahwa algoritma ini mempunyai nilai korelasi yang cukup rendah antara plainteks dan cipherteks. Modifikasi *Hill Cipher* juga dapat menahan serangan kriptanalisis *known plaintext attack* (KPA).

Kata Kunci: *Hill Cipher*, Kriptografi, Matriks, Inisial Permutasi, Lotre, *Known Plaintext Attack*

[1] Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.
[2] Staff Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.